PCT/IB 0 4 / 0 1 3 0 2
(1 7. 05. 04).

PA 1165192

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

May 05, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/455,615***
FILING DATE: ***March 18, 2003***

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

L. Edelen

L. EDELEN
Certifying Officer

BEST AVAILABLE COPY

03-19-03 60455615.03/18/03

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Express Mail Label No. EV 249512500US

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
GUILLAUME	BICHOT	PRINCETON, NJ, US

☐ *Additional inventors are being named on the _____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

A 3GPP/GPRS SIGNALING CONNECTION MANAGEMENT COMPATIBLE WITH THE IEEE802.1X MODEL

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number
OR
Type Customer Number here → *Place Customer Number Bar Code Label here*

☒ Firm or Individual Name	JOSEPH S. TRIPOLI, THOMSON MULTIMEDIA LICENSING INC..				
Address	PATENT OPERATIONS.				
Address	P. O. BOX 5312				
City	PRINCETON	State	NJ	ZIP	08543-5312
Country	USA	Telephone	609-734-6834	Fax	609-734-6888

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 8 ☐ CD(s), Number ____

☐ Drawing(s) *Number of Sheets* ____ ☐ Other (specify) ____

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees

FILING FEE AMOUNT ($): 160

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 07-0832

☐ Payment by credit card. Form PTO-2038 is attached.

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒No.

☐Yes, the name of the U.S. Government agency and the Government contract number are: _____.

Respectfully submitted, SIGNATURE Paul P. Kiel	Date: *March 18, 2003*
TYPED or PRINTED NAME PAUL P. KIEL	REGISTRATION NO. 40,677 *(if appropriate)*
TELEPHONE 1 609 734 6815	Docket Number: PU030087

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

Express mail: EV249512500 US PU030087

A 3GPP/GPRS Signaling connection management compatible with the IEEE802.1X model

In the context of inter-working between a 3GPP/GPRS network and a public WLAN, the MT (Mobile Terminal) interacts with its counter part in the 3GPP network for control purpose. This control flow gathers information relative to the authentication procedure among other information. It is envisaged to use the EAP protocol combined with a dedicated WLAN procedure (IEEE 802.1X for instance). These procedures terminate normally once the MT and the network are mutually authenticated. Consequently maintaining alive an EAP connection is against the standardization and may be impossible to do (the access point could blocked further EAP traffic). The invention proposes a way to continue the signaling flow by switching the signaling connection over an alternative transport mechanism.

The development of public WLAN access network is growing. Since it is impossible for a user to subscribe to all different WLAN operators. There are some service providers acting as virtual WLAN operators that aggregate, in some way, several WLAN by setting agreement with the different WLAN operators.

A service provider may be a cellular network (3GPP) operator. In that case the cellular operator may propose two types of service for a customer.
An Internet access only service where the user is authenticated by the cellular network and is then authorized to access the Internet through the WLAN (the data never go through the cellular network but only the control information for authentication, authorization and accounting). This way to do is called "loose coupling" because the data path never go through the cellular network.
The second type of service is a full cellular network access from the WLAN (this include also the Internet access but through the cellular network). This service requires sending control information and data to the cellular network. The WLAN is acting as the radio network part of the cellular network. This way to do is called "tight coupling". This solution brings some obvious advantages to the user and the cellular network operator.

Today, the different standard bodies focus on the so-called loose coupling model that solved the AAA (Authentication, Authorization, Accounting) issue. The architecture is based on a security model like IEEE802.1X that requires the support of EAP and a remote security server supporting RADIUS or DIAMETER. The authentication protocol can change depending on the type of MT. The tendency is to use a new authentication protocol compatible with the SIM card present in a 3GPP MT. This way to do ignores completely the protocols already existing in the 3GPP/GPRS architecture. For Authentication, there is already a procedure well specified and used by millions of portable devices called GMM. Moreover there are other 3GPP/GPRS procedures in order to manage data streams for instance. By ignoring voluntary existing 3GPP/GPRS protocols, the working group is reinventing the wheel. One argumentation given by the people in favor of redefining new protocols is that there is no possibility to carry signaling over EAP since EAP has to be used only for authentication.

This invention proposes a mechanism to switch the signaling connection from an EAP transport mechanism to another transport mechanism.

References

[1] **Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2 (3GPP TS 23.060 version 3.7.0 Release 1999)**

Introduction

This paper presents a solution to maintain a signaling connection while changing the transport protocol. In the context of a WLAN interworking with a 3G cellular network, the WLAN architecture has to support a well defined and probably broadly support mechanism called remote authentication. This mechanism is specified by the IEEE 802.1X and adapted to the IEEE 802.11 WLAN technology whereas an equivalent mechanism is specified for the ETSI/Hiperlan2 WLAN technology. Authentication protocol is one of the signaling protocols that take place between the MT (Mobile Terminal) and the cellular network (UMTS/GPRS). However there are other control protocols to manage the data flow for instance that need to be carried over a signaling connection. Using EAP and EAPOL (IEEE 802.1X) is restricted to the authentication phase. There is a need to maintain the signaling connection alive in order to be able to carry subsequent signaling phase that take place during the attachment of the mobile terminal with the cellular network.

The 3G (UMTS) Network

The architecture of GPRS 3G network is depicted in the figure 1. It is basically composed with a radio access network (RAN) and a core network (CN). The radio access network gathers a set of Radio Network Controllers (RNC) each RNC controlling a set of node B. A node B is also called base station and gather the antenna that relay the signal from to the mobile terminal. A node B corresponds to a cell. In the Core Network (CN) the SGSN (Serving GPRS Support Node) provides the services for managing the connection between the CN and the user (connection, authentication, mobility). The SGSN serves as a front end for other 3G services like SMS (Short Messaging System). The GGSN (Gateway GPRS Support Node) provides the inter-connection between the CN and an external network that is an IP based network (Internet for instance). The HLR (Home Location Register) is the database that contains all information relative to a subscriber. Last, the BG (Border Gateway) is a function that allows roaming between GPRS networks belonging to different domains (operators).

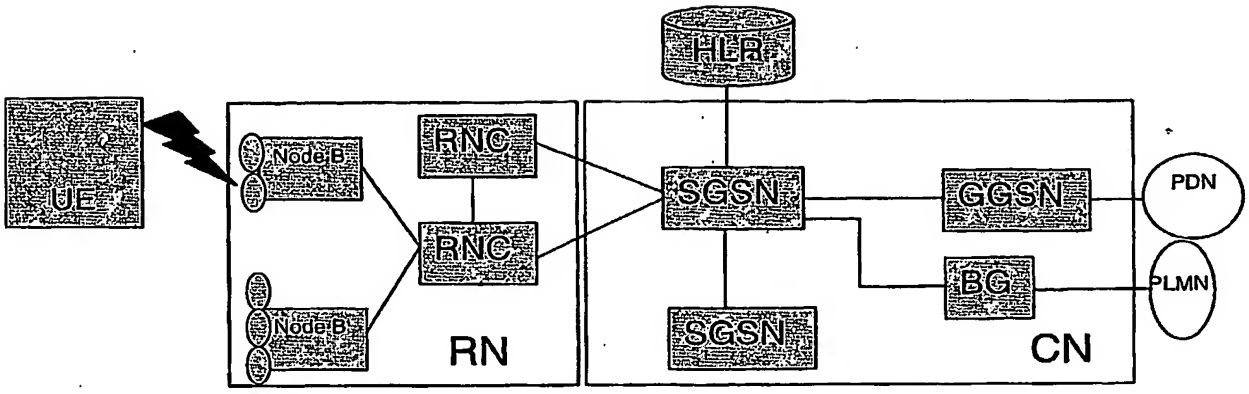

Figure 1 - 3G GPRS architecture

Looking at the figure 2 The RNC realizes the interface between the core network and the radio network. When the mobile terminal requests a connection through the CM (Connection Management) protocol, the SGSN processes the request and requests through the RANAP (Radio Access Network Protocol) the RNC to establish the radio part of the connection. The RNC translates the request into parameters used to establish the corresponding radio connection and delivers these parameters to the UE through the RRC (Radio Resource Control) protocol. The UE RRC uses these parameters to configure its radio protocol layers (RLC, MAC, physical).

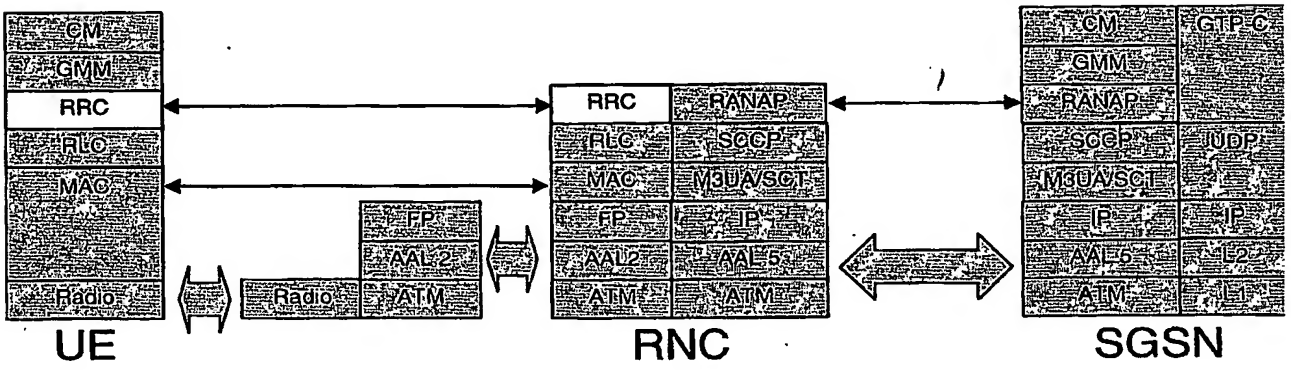

Figure 2 - 3G GPRS Control protocol stack

A protocol stack based on ATM carries RANAP.
The figure 3 depicts the user data protocol stack. The user data (IP for instance) is transported using the PDCP (Packet Data Compression Protocol) that consists to compress the IP header in order to economize some bandwidth. Between the RNAC and the SGSN and within the rest of the core network (up to the GGSN not represented in the figure 3) GTP (GPRS Tunnel Protocol) that is implemented over UDP/IP carries the user data.

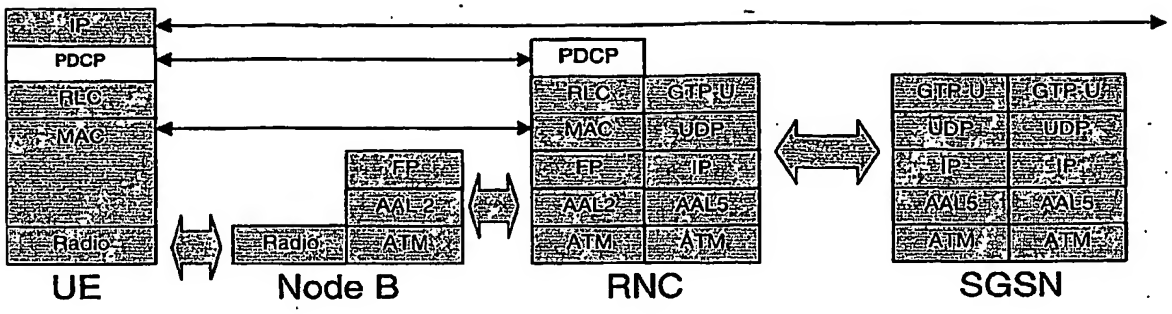

Figure 3 - 3G GPRS User data protocol stack

The Loose coupling model

The following drawing (Figure 4) shows a loose coupling scenario as the different standard bodies envisage it. A user that is a 3G-network subscriber is in the coverage of a WLAN. Once the user switches on his mobile terminal, the WLAN will redirect the connection request towards an AAA (Authentication Authorization and Accounting) server. After being authenticated, the AAA authorizes the WLAN (the access point) to let go the user data traffic through the access point. The user is then able to browse the Internet. By loose coupling we mean that the data path never goes through the 3G-core network. There is thus no need to signaling flow between the MT and the 3G-core network other than this related to authentication.

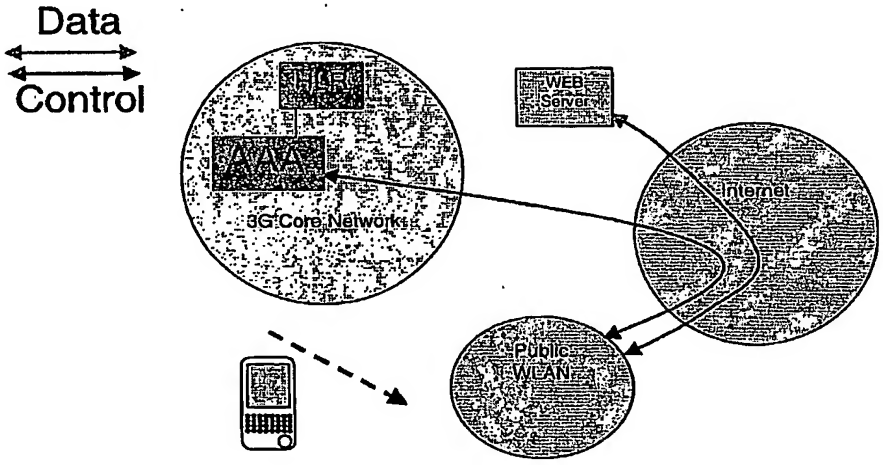

Figure 4 - Cellular 3G- WLAN "Loose coupling "solution

The protocol stack that is envisaged in the mobile terminal, in the AP (Access Point) and in the AAA server is represented in the figure 2.

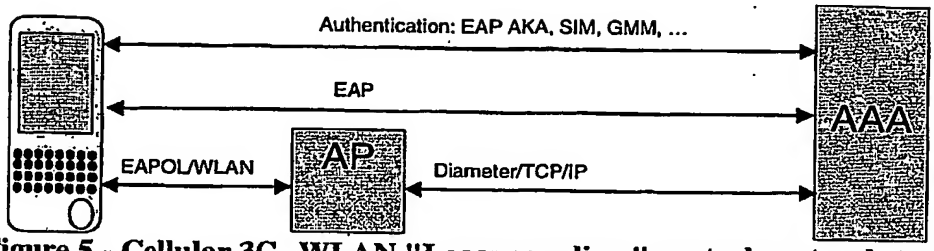

Figure 5 - Cellular 3G- WLAN "Loose coupling " control protocol stack

The figure 5 assumes IEEE 802.11 as the radio interface between the mobile terminal and the AP but it can be also other WLAN protocols like the ETSI Hiperlan2 protocol.
EAPOL (meaning EAP Over LAN) is a standardized (IEEE 802.1X) protocol that is used to carry EAP packets within Ethernet frames. The AP blocks any Ethernet frame except those carrying EAPOL until the user is authorized (signaled by the AAA through DIAMETER).
EAP (meaning Extended Authentication Protocol) is a simple IETF protocol used to carry any kind of authentication protocol. The authentication protocol may be any kind as, for instance the EAP AKA and EAP SIM that might be chosen by the 3GPP standard body. The authentication protocol could also be the GMM (GPRS Mobility Management) protocol currently used by 3GPP and that gather an authentication procedure. The DIAMETER protocol is a well-known IETF protocol used to control the authorization of the user by the AAA. Once the user is authenticated (the AAA server retrieved a corresponding entry in its subscription database and the authentication protocol succeeded), the AAA server sends a DIAMETER message to the AP in order to unblock the Ethernet traffic corresponding to the authenticated user.

The user plane stack is simply IP over Ethernet over the WLAN MAC (IEEE 802.11 in our example).

The tight coupling model

The tight coupling model is based on the previous model. However, the data path goes through the cellular network as well. The obvious advantage is that the MT can access to the cellular 3G core network specific services like IMS, SMS and so on. Another advantage is that it simplifies the relationship between the WLAN operator and the cellular network operator since the accounting can be verify by the 3G-core network operator.

The figure 6 presents the tight coupling model supported by the invention.

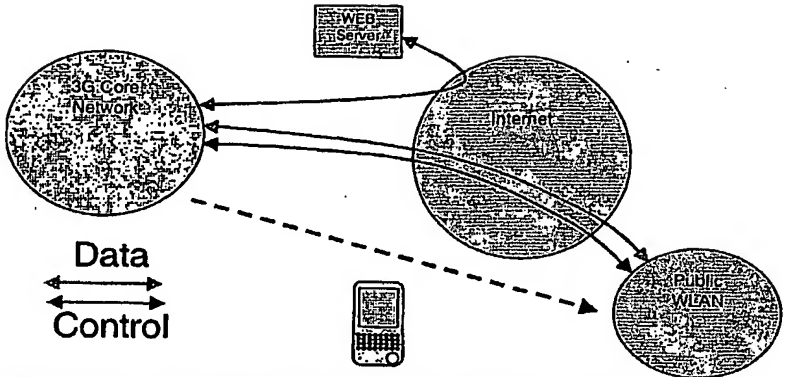

Figure 6 - Cellular 3G- WLAN "Tight coupling "solution

The controls and the data go through the cellular 3G-network. The data stream as well as the control support Internet protocols as depicted in the following section.

Protocol stacks for tight coupling

The disclosure PU030056 entitled "A 3G GPRS - WLAN TIGHT COUPLING SOLUTION USING INTERNET" filed as a U.S. provisional application on February 27, 2003, introduces what could be the protocol stack in both the MT and the 3G-core network gateway (SGSN) for a tight coupling solution. That solution is based on a signaling flow permanently transported by the EAP/EAPOL connection as refreshed by the following figure.

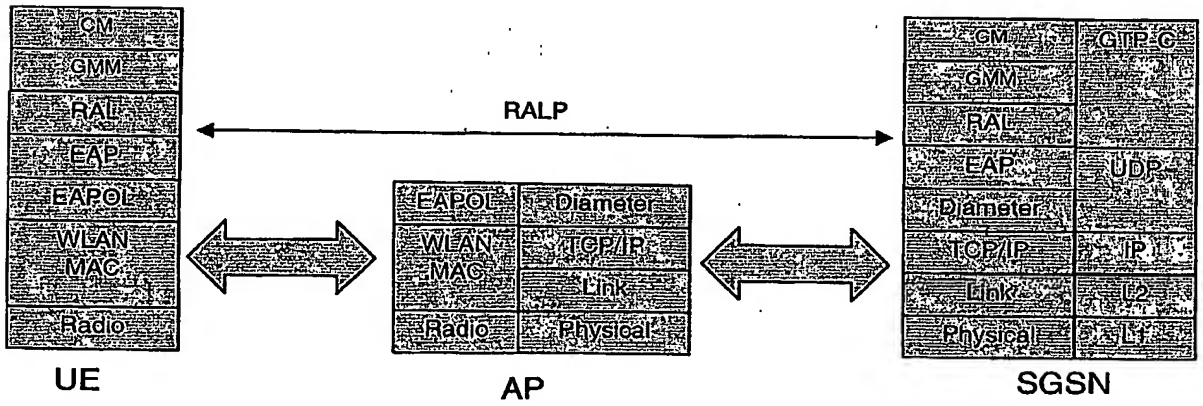

Figure 7- Cellular 3G- WLAN "Tight coupling " Control plane

The RAL (Radio Adaptation Layer) and RALP protocol is the subject of the PU030056 disclosure.

When a mobile terminal moves in a WLAN or when a mobile terminal is switched on in a WLAN, it first establishes an EAP connection with a remote AAA server (the SGSN in our case) in conformance with the remote authentication procedure specified by IEEE802.1X (see figure 5). The AP authorizes only the EAP traffic. The UE is then authenticated according to the 3G GPRS protocol (GMM). Once it is authenticated, the SGSN authorizes the user by sending a DIAMETER message to the access point (AP).

The RALP protocol provides extra signaling procedures and conveys other signaling procedures like the Connection Management (CM) in order to establish user data flows.

The figure 8 shows the user data protocol stack.

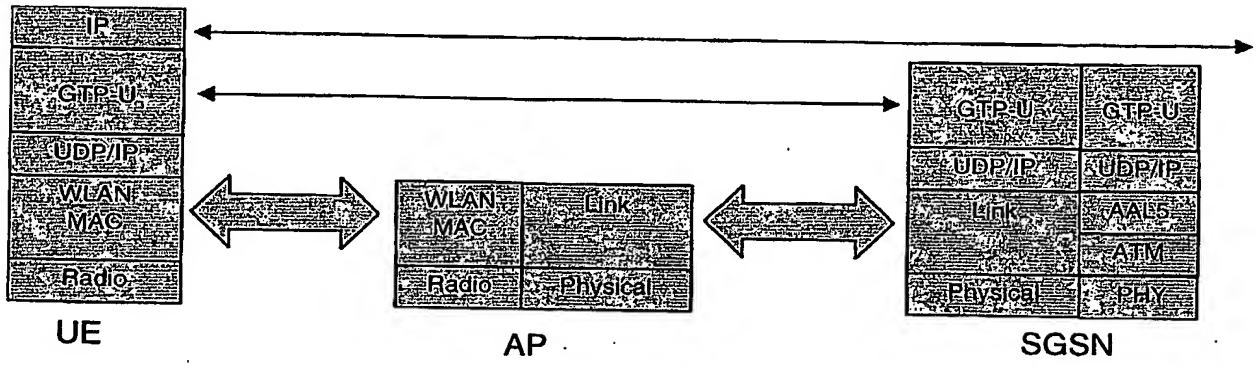

Figure 8- WLAN interfaces - User plane

What we see here is that the user data is carried over a tunnel that permits to cross intermediate networks (between the AP and the SGSN) that could be Internet. This tunnel could be compliant with different method. Our choice here is GTP that is already supported by the 3GPP core network. The usage of another tunneling mechanism is possible like Ip over Ip.

Signaling connection initialization

PU030056 assumption is that the signaling connection is initialized using EAP over EAPOL (for IEEE 802.11) and remains alive even after the authentication is done. As explained above, this situation is not compliant with the spirit of the EAP specification (RFC 2284), it can cause problems with the underlying radio dependant mechanism (EAPOL), it can be quite inefficient by consuming EAPOL resources continuously and it is not flexible (signaling radio resources could also required some QOS that is not possible with the EAPOL.
What it is proposed here is to switch the initial signaling connection over another transport mechanism. Once the authentication phase is done, the cellular network gateway (SGSN) delivers to the Mobile Terminal (MT) the necessary parameters in order to open a new tunnel (GTP for instance) dedicated to signaling flow.

The following figure (figure 9) presents what should be the signaling flow regarding this new procedure.

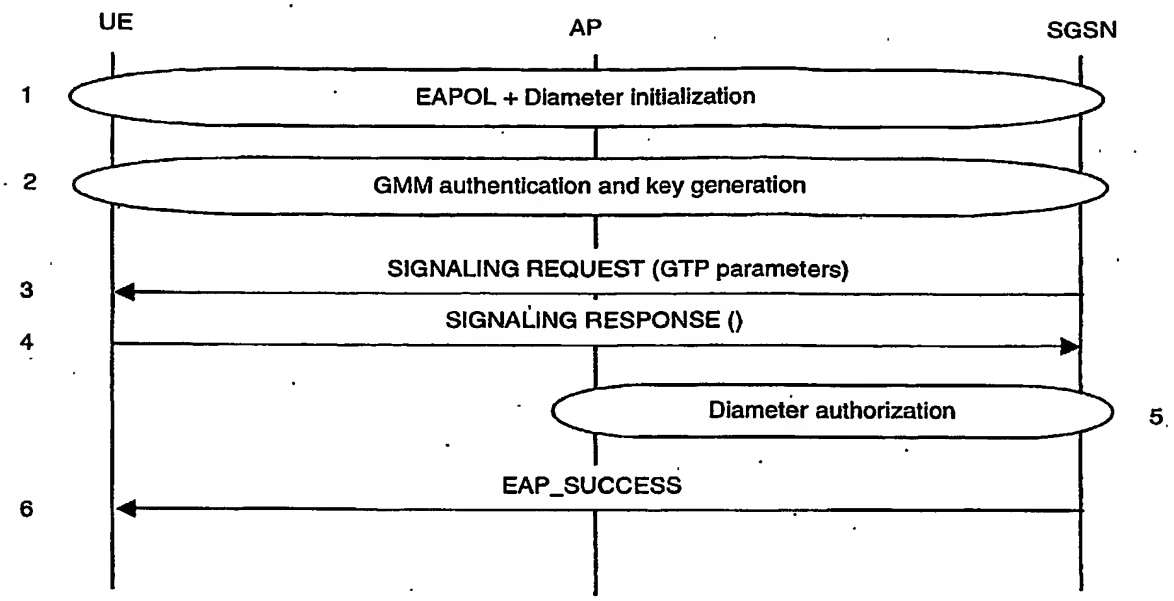

Figure 1 - Initial RALP connection

1. The EAPOL (or an equivalent radio mechanism) is established between the MT and the AP, the DIAMETER connection is established between the AP and the SGSN and an end-to-end EAP session is set up in conformance with the remote authentication mechanism specified by IEEE 802.1X/IEEE 802.11.
2. The authentication procedure may be performed. All the signaling traffic goes through EAP over EAPOL (over the radio interface) and EAP over DIAMETER (over the wired interface including Internet)
3. Once the MT is authenticated, The SGSN delivers to the MT the necessary information to continue to carry signaling messages over a dedicated GTP tunnel. The MT can thus reserve radio resource if necessary (when QOS is possible) and establishes the tunnel (GTP or other technique can be used) with the remote SGSN.
4. The UE acknowledges the previous command and in case of success.
5. The SGSN authorizes the access point (using DIAMETER protocol) to let the user data traffic related to the MT going through.
6. The SGSN signal the success of the authentication according to the EAP protocol. The MT closes its EAPOL/EAP connection and open the new tunnel according to the parameters provided by the SGSN (for GTP, the parameters are basically an IP address, a tunnel ID and some potential QOS parameters). The subsequent signaling traffic flows through the new tunnel.

Advantages of the invention

The mechanism presented here above provides a way to establish and maintains a signaling connection alive, according to the 3GPP/GPRS protocol stack requirements, being compliant with the remote authentication model illustrated by the IEEE802.1X mechanism.

This Page is inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox